Maine State Government
Dept. of Administrative & Financial Services
Office of Information Technology (OIT)

Procedure for SecurID Cards and Maintenance of the RSA Database

1.0 Purpose

State agencies will comply with this procedure when acquiring *SecurID cards*. Security Coordinators will comply with this procedure for maintaining accountability for SecurID cards. The purpose of this procedure is to govern the accountability and procedures for SecurID cards.

2.0 Definitions

2.1 **Agency Supervisor(s)**: A Supervisor or Manager within the Agency who can authorize the purchase of a SecurID card and can grant an Employee use of a SecurID card.

2.2 **Call Center Specialist**: The person at the Call Center who fulfills the requests submitted by the *Security Coordinator* or designated person.

2.3 **RSA Database**: RSA Access Manager software enables organizations to manage large numbers of users while enforcing a centralized security policy that ensures compliance, protects enterprise resources from unauthorized access, and makes it easier for legitimate users to do their jobs.

2.4 **SecurID card**: To access resources protected by the RSA SecurID system, users simply combine their Personal Identification Number (PIN) (something they alone know) with the token codes generated by their authenticators (something they have). The result is a unique, one-time-use passcode that is used to positively identify, or authenticate, the user, with "two-factor" authentication. If the code is validated by the RSA SecurID system, the user is granted access to the protected resource. If it is not recognized, the user is denied access. RSA stands for Rivest, Shamir, Adelman, the inventors of this encryption technique.

2.5 **SecurID Program Administrator**: The person at the Call Center who administers the *RSA database*, and assures that all policies and procedures are followed according to the SecurID Card procedure and processes.

2.6 **Security Coordinator**: Person, designated by the Agency, to manage the ordering of new and expired SecurID cards through a report sent to them each month from the SecurID Program Administrator.

2.7 **Semi-autonomous State Agency**: An Agency created by an act of the Legislative Branch that is not a part of the Executive Branch. This term does not include the Legislative and Judicial Branches, Offices of the Attorney General, Secretary of State, State Treasurer, and Audit Department.

3.0 Applicability

This is intended to manage the process of acquiring and accountability of SecurID cards for: Employees and Contractors of Agencies within the Executive Branch and *semi-autonomous State Agencies*.

4.0 Responsibilities

4.1 *Agency Supervisor(s)* (or designees) approve SecurID card requests and the cost of that card.

4.2 Security Coordinators, working with the Agency Supervisors, request online SecurID cards for Contractors and all State Employees.

4.3 The *SecurID Program Administrator* ensure that all aspects of the SecurID card program are followed in accordance with this procedure.

5.0 Directives

5.1 SecurID Program Administrator

5.1.1 Maintains the overall supervision of this program and keep all procedures current and up to date.

5.1.2 Ensures that an adequate number of SecurID cards are available to fulfill requests.

5.1.3 Maintains Security Coordinator list and distribute to *Call Center specialist*.

5.1.4 Ensures that this list is verified semi-annually with the agencies.

5.1.5 Provides SecurID card holders list to each of the Security Coordinators for their perspective agencies, monthly.

5.1.6 Generates a monthly inactivity report for Contractor card holders greater than 120 days. Provide this list to the Security Coordinators and inform them that these cards will be disabled. Disable all 120 day or greater inactive Contractor card users.

5.2 Security Coordinator

5.2.1 Provides the Call Center with a request for the SecurID card via the request form http://footprints.state.me.us/footprints/rsa.html (If you have not been set up for this web site and would like to be, call 624-7700 and one of the Call Center staff can set you up with a user name and password) or put a ticket in via the Footprints portal: https://footprints.state.me.us/footprints

5.2.2 Reviews end of month report to determine if a SecurID card is needed for cards expiring and that all users are valid.

5.2.3 Upon notification from users that have been disabled, verifies their status and contact the Call Center for placement into active status.

5.2.4 Notifies SecurID Program Administrator of any changes to Security Coordinator assignments.

5.2.5 If a contractor leaves the State, ensures that the agency completes a Delete User form, which is under the User Request project within Footprints.

5.3 Call Center Specialist

5.3.1 When the Call Center receives a SecurID request, completes the request, utilizing the standard operating procedure for fulfilling SecurID requests.

5.3.2 For users calling in that are unable to login and have verified that they have been disabled for inactivity due to multiple logon attempts, re-enables their login. If they have not logged into the system within 120 days or more, then have those users contact their Security Coordinator for re-activation of their card.

5.3.3 Disables accounts for contractors no longer working for the State, as directed by the Agency.

6.0 Document Information

Initial Issue Date: May 1, 2009
Last Revision Date: April 10, 2019 – To update Document Information.

Point of Contact: Security Compliance and Policy Manager, OIT.Policy-Compliance@Maine.Gov
Approved By: Chief Information Officer, OIT
Enforced By: Chief Information Officer, OIT

Legal Citation: Title 5, Chapter 163: Office of Information Technology[1]
Waiver Process: See the Waiver Policy[2].

[1] http://legislature.maine.gov/statutes/5/title5ch163sec0.html
[2] http://maine.gov/oit/policies/waiver.pdf